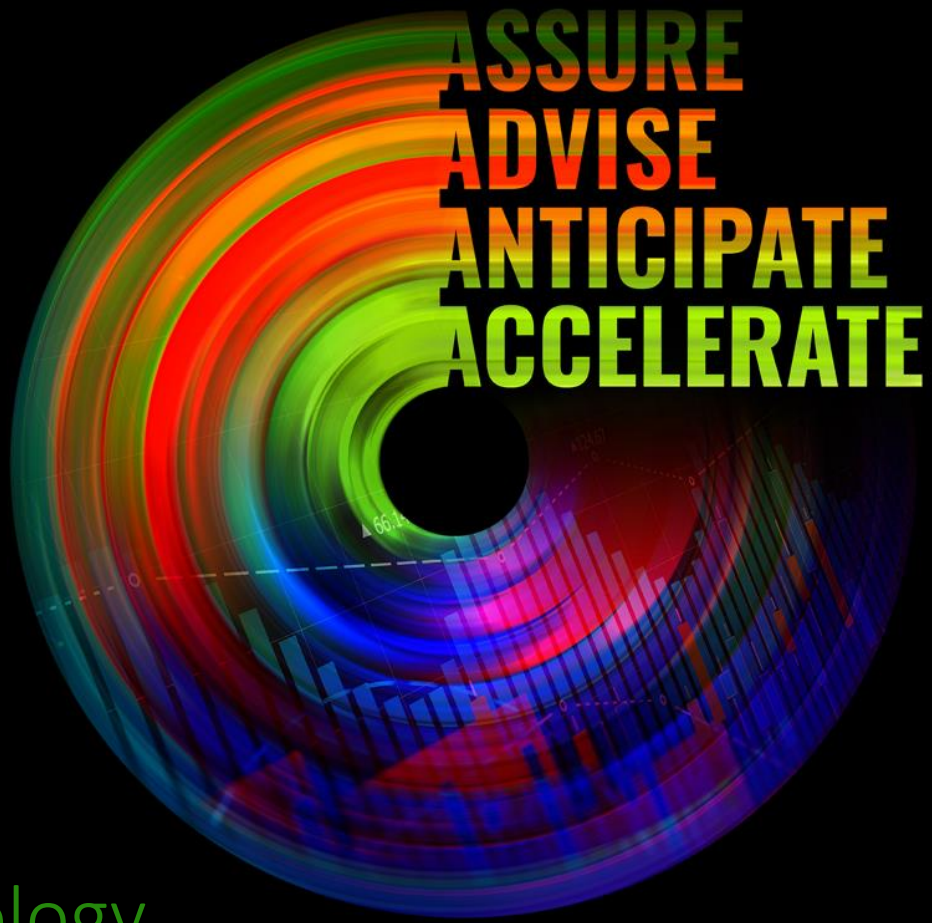
Deloitte.



How to Audit Technology and Cyber Risk

Navigating Risk Management in Technology (RMiT)

MAKING AN IMPACT THAT MATTERS since 1845

Bank Negara Malaysia's (BNM) Risk Management in Technology

RMiT contains BNM's requirements for organisations to follow in managing technology and cyber risks matters effectively and aims to achieve the following objectives:


BANK NEGARA MALAYSIA
CENTRAL BANK OF MALAYSIA

Risk Management in Technology (RMiT)

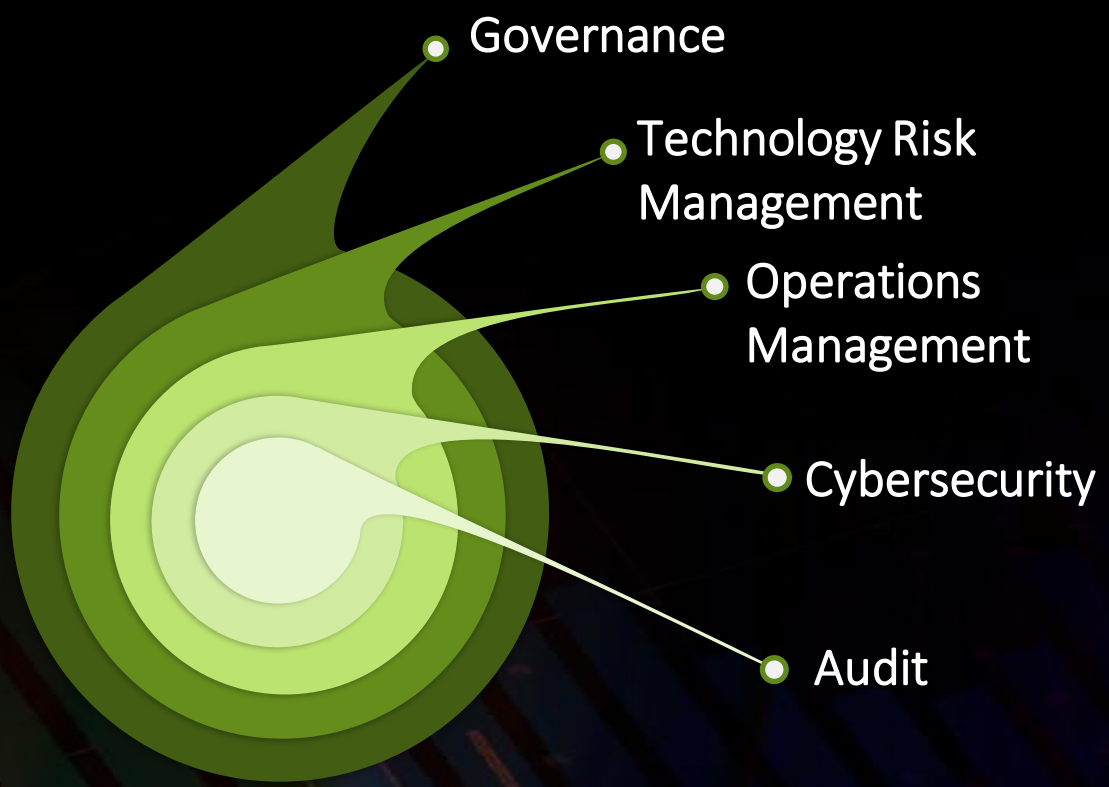
Applicable to:
1. Licensed banks, including licensed digital banks
2. Licensed investment banks
3. Licensed Islamic banks, including licensed Islamic digital banks
4. Licensed insurers including professional reinsurers
5. Licensed takaful operators including professional retakaful operators
6. Prescribed development financial institutions
7. Approved issuers of electronic money
8. Operator of a designated payment system

Issued on: 01 June 2023 BNM/RH/PD 028-98

- Section 8: Governance over technology & cyber risk
- Section 9: Effective technology risk management
- Section 10 & 11: Ensure robust technology and cyber controls
- Section 12: Effective internal audit program

RMiT's Key Focus Areas

RMiT's Focus Areas contributes to the effectiveness of cyber risk management and operations within your organisation.



BNM's RMiT guidelines encompass a holistic approach to managing technology risks. It emphasize **Governance** by outlining clear roles and responsibilities for managing these risks.

Technology Risk Management involves establishing a framework for identifying, assessing, and mitigating these risks through various measures.

Operations Management focuses on ensuring secure and efficient IT operations.

Cybersecurity is a critical aspect, demanding robust controls to safeguard against cyber treats and vulnerabilities.

The guidelines also stresses the importance of regular **Audits** to assess the effectiveness of implemented controls.

A view on the landscape

Our experience with RMiT has provided us with relevant context on the common challenges faced by Internal Audit in navigating RMiT.

Evolving Cyber Threats necessitate continuous updates to security measures and staying abreast of the latest attack vectors.

Data Security And Privacy are paramount, as financial institutions hold sensitive customer information and must comply with relevant data protection regulations.

Third-party Risk Management is crucial, as reliance on external vendors introduces additional vulnerabilities that require careful assessment and mitigation strategies.

Cloud Adoption Security warrants close attention, as leveraging cloud services necessitates robust security controls and careful selection of cloud providers.

Compliance Fatigue can hinder the effectiveness of risk management, emphasizing the need for well-defined frameworks and efficient compliance processes.

Addressing Internal Audit's cyber needs

Here's how we can help you navigate the complexities of RMiT:

1. Audit on System/Application Material Enhancements
2. Audit on your Cloud Adoption and Implementation Strategies
3. Audit via Red Team Exercises
4. Audit on Cyber Security Compliance:

   Cyber Policies and Procedure / Cyber Operations and Implementation
5. Audit on Third Party Cyber Risk
6. Audit on the Data Center Security and Network Resiliency

With a track record of assisting various Internal Audit functions in Malaysia, we embrace a proactive approach to **identify non-compliances**, help **develop robust initiatives** of improvement, and bring you industry best practices and knowledge to execute an **effective internal audit program** on RMiT compliance.

Key questions for Internal Audit to consider

Cyber raises tough questions.
We provide the answers.

Governance
What proactive measures have the Board & Senior Management implemented to ensure that your IT and cyber strategic plans continuously address emerging threats and remain on top of technological advancements?

Technology Operations Management
Beyond the established frameworks and policies, how effectively are your daily cybersecurity practices translated into tangible actions that continuously identify, prevent, and mitigate cyber threats to your operations?

Technology Audit
How do you ensure that your technology audit function has specialised technology audit competencies and is supported by skilled and experience resources?

Technology Risk Management
To what extent are the current TRMF and CRF effectively safeguarding your organisation's information infrastructure, systems, and data, while ensuring continuity of operations and delivery of financial services?

Cybersecurity Management
How does your organization determine that the cybersecurity tools that you have deployed are operated and managed effectively?

Internal Awareness and Training
How effective is the periodic technology and cybersecurity awareness programs in your organization?

Success Stories

Speak with us to know more about our experience with RMiT.

01

Foreign Financial Institution

Context: The organization was to undertake a technology refresh. However, complying with RMiT guidelines, which mandates a thorough external service provider (ESP) assessment for multiple systems presented a significant challenge.

Our Value Delivered: We embarked on a multi-year engagement to assist and facilitate the organization's attestation process for material enhancement, ensuring applications can go-live in a timely manner.

02

Local Financial Institution

Context: The organization required assistance to align the TRMF and CRF documents with RMiT and standard best practices.

Our Value Delivered: We brought references of framework documents from our local and global resources to give insights into the standard of frameworks that were developed with efficiency and practicality in mind.

03

Foreign Financial Institution

Context: The organization required visibility on the new iteration of RMiT, specifically on their compliance towards Cloud Adoption.

Our Value Delivered: We brought together a team of Cloud Subject Matter Experts who were able to provide the organization with relevant context and insights on the gaps in their cloud journey and the initiatives that they can embed to be ready to move to cloud.

Let’s Talk

How we can help

Overcoming RMiT Compliance Hurdles: Let Deloitte Be Your Cybersecurity Partner

Navigating the complexities of RMiT compliance can be a significant challenge for organizations lacking the necessary expertise in cybersecurity and technology. Our team understands these challenges and is here to assist you in achieving comprehensive RMiT compliance through a fully outsourced audit program or a co-sourcing Internal Audit support program.

Through our approach, we can equip your team with the necessary skills and knowledge to confidently navigate RMiT compliance on their own with comprehensive trainings designed to address your organization's specific needs and RMiT requirements, as well as knowledge transfer exercises to ensure your team gains a deep understanding of the RMiT framework and best practices through interactive exercises and hands-on experience.

Get in touch

Ho Siew Kei
Executive Director
Deloitte Risk Advisory
sieho@deloitte.com

Adriel Hing
Director
Deloitte Risk Advisory
ahing@deloitte.com

Deloitte.